What is claimed is:

1. A method for protecting a file system in a computer, wherein a user having an access authority for a file can access the file system in the computer, the method comprising the steps of:

a) generating system security manager's digital signature keys and system security manager's certificate;

b) storing system security manager's certificate onto a security kernel when installing an operating system on a server computer;

c) generating second digital signature keys and user's certificate;

d) setting an access authority of the file system;

e) identifying a user through a digital signature based authentication when the user tries to access the file system; and

f) giving the user the access authority for the file in accordance with identification result.

2. The method as recited in claim 1, further comprising the step of g) performing a user registering/deleting process if the user is identified as the system security manager.

3. The method as recited in claim 1, further comprising the step of h) setting the access authority of the file system if the user is identified as the system security manager.

4. The method as recited in claim 1, further comprising the step of i) accessing and processing a file.

5. The method as recited in claim 1, wherein the step a) includes the steps of:

a-1) generating a system security manager's public

key;

a-2) generating a system security manager's secret key; and

a-3) generating system security manager's certificate.

6. The method as recited in claim 1, wherein the step e) includes the steps of:

e-1) generating, at a server computer, random numbers;

e-2) generating a digital signature to the random number;

e-3) extracting system security manager's public key from system security manager's certificate stored on the security kernel;

e-4) verifying user's certificate by system security manager's public key extracted;

e-5) extracting user's public key and the access authority in user's certificate; and

e-6) verifying the digital signature to the random number.

7. The method as recited in claim 1, wherein the step f) includes the steps of:

f-1) providing the user with the file system access authority to the file system if the user is the general user; and

f-2) providing the user with registering/deleting authority, file system access setting authority and the file system access authority.

8. The method as recited in claim 2, wherein the step g) includes the steps of:

g-1) determining whether user registration or deletion is selected;

g-2) deleting data related to a user to be deleted if the user deletion is selected;

g-3) registering a user if the user registration is

selected;

wherein the step g-3) includes the steps of:

g-3-1) providing the user to be registered with the access authority;

g-3-2) generating a secret key and a public key of the user to be registered;

g-3-3) generating a certificate of the user to be registered;

g-3-4) encrypting and storing the secret key of the user to be registered; and

g-3-5) storing the certificate of the user to be registered.

9. The method as recited in claim 8, wherein the certificate is generated by encrypting the access authority and user's public key.

10. The method as recited in claim 3, wherein the step h) includes the steps of:

h-1) selecting a file;

h-2) selecting a user allowed to be access the file; and

h-3) setting the access authority to the file as an access authority of the user.

11. The method as recited in claim 4, wherein the step i) accessing and processing a file includes the steps of:

i-1) receiving a name of a file to be accessed;

i-2) determining whether an access authority of the file to be accessed is equal to that of the system security manager;

i-3) permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the system security manager;

i-4) determining whether the access authority of the file to be accessed is equal to that of the user trying to

access thereto; and

i-5) permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the user trying to access thereto.

12. An apparatus for protecting a file system in a computer system, wherein a user having a file access authority can access the file system in the computer system, the method comprising:

means for generating system security manager's digital signature keys and system security manager's certificate;

means for storing system security manager's certificate onto a security kernel when installing an operating system on a server computer;

means for generating user's digital signature keys and user's certificate;

means for setting an access authority of the file system;

means for identifying a user through a digital signature authentication method when the user tries to access the file system; and

means for giving the user the access authority for the file in accordance with identification result.

13. The apparatus as recited in claim 12, further comprising means for performing a registration/deletion of the user if the user is identified as the system security manager.

14. The apparatus as recited in claim 12, further comprising means for setting the access authority of the file system if the user is identified as the system security manager.

15. The apparatus as recited in claim 12, further comprising means for accessing and processing a file.

16. The apparatus as recited in claim 12, wherein the means for generating system security manager's digital signature keys and system security manager's certificate includes:

means for generating system security manager's public key;

means for generating system security manager's secret key; and

means for generating system security manager's certificate.

17. The apparatus as recited in claim 12, wherein the means for identifying a user includes:

means for generating, at a server computer, random numbers;

means for generating a digital signature to the random number;

means for extracting system security manager's public key from in system security manager's certificate stored on the security kernel;

means for verifying user's certificate by system security manager's public key extracted;

means for extracting user's public key and the access authority in user's certificate; and

means for verifying the digital signature to the random number.

18. The apparatus as recited in claim 12, wherein the means for giving the user the access authority includes:

means for providing the user with the file system access authority to the file system if the user is the general user; and

means for providing the user with registering/deleting authority, file system access setting authority and the file system access authority.

19. The apparatus as recited in claim 13, wherein the means for performing a registration/deletion of the user step g) includes:

means for determining whether user registration or deletion is selected;

means for deleting data related to a user to be deleted if the user deletion is selected;

means for registering a user if the user registration is selected;

wherein the means for registering a user includes:

means for providing the user to be registered with the access authority;

means for generating user's secret key and public key to be registered;

means for generating user's certificate to be registered;

means for encrypting and storing user's secret key to be registered; and

means for storing user's certificate to be registered.

20. The apparatus as recited in claim 19, wherein user's certificate is generated by encrypting the access authority of the user and user's public key.

21. The method as recited in claim 14, wherein the means for setting an access authority includes the steps of:

means for selecting a file;

means for selecting a user allowed to be access the file; and

means for setting the access authority to the file as an access authority of the user.

22. The method as recited in claim 15, wherein the means for accessing and processing a file includes:

means for receiving a name of a file to be accessed;

means for determining whether an access authority of the file to be accessed is equal to that of the security manager;

means for permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the security manager;

means for determining whether the access authority of the file to be accessed is equal to that of the user trying to access thereto; and

means for permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the user trying to access thereto.

23. A computer readable media storing instructions for executing a method for protecting a file system in a computer, wherein a user having an access authority for a file can access the file system in the computer, the method comprising the steps of:

a) generating system security manager's digital signature keys and system security manager's certificate;

b) storing system security manager's certificate onto a security kernel when installing an operating system on a server computer;

c) generating second digital signature keys and user's certificate;

d) setting an access authority of the file system;

e) identifying a user through a digital signature based authentication when the user tries to access the file system; and

f) giving the user the access authority for the file in accordance with identification result.

24. The computer readable media as recited in claim 23, wherein the method further comprises the step of g) performing a user registering/deleting process if the user

is identified as the system security manager.

25. The computer readable media as recited in claim 23, wherein the method further comprises the step of h) setting the access authority of the file system if the user is identified as the system security manager.

26. The computer readable media as recited in claim 23, wherein the method further comprises the step of i) accessing and processing a file.

27. The computer readable media as recited in claim 23, wherein the step a) includes the steps of:

a-1) generating a system security manager's public key;

a-2) generating a system security manager's secret key; and

a-3) generating system security manager's certificate.

28. The computer readable media as recited in claim 23, wherein the step e) includes the steps of:

e-1) generating, at a server computer, random numbers;

e-2) generating a digital signature to the random number;

e-3) extracting system security manager's public key from system security manager's certificate stored on the security kernel;

e-4) verifying user's certificate by system security manager's public key extracted;

e-5) extracting user's public key and the access authority in user's certificate; and

e-6) verifying the digital signature to the random number.

29. The computer readable media as recited in claim 23, wherein the step f) includes the steps of:

f-1) providing the user with the file system access authority to the file system if the user is the general user; and

f-2) providing the user with registering/deleting authority, file system access setting authority and the file system access authority.

30. The method as recited in claim 24, wherein the step g) includes the steps of:

g-1) determining whether user registration or deletion is selected;

g-2) deleting data related to a user to be deleted if the user deletion is selected;

g-3) registering a user if the user registration is selected;

wherein the step g-3) includes the steps of:

g-3-1) providing the user to be registered with the access authority;

g-3-2) generating a secret key and a public key of the user to be registered;

g-3-3) generating a certificate of the user to be registered;

g-3-4) encrypting and storing the secret key of the user to be registered; and

g-3-5) storing the certificate of the user to be registered.

31. The computer readable media as recited in claim 30, wherein the certificate is generated by encrypting the access authority and user's public key.

32. The computer readable media as recited in claim 25, wherein the step h) includes the steps of:

h-1) selecting a file;

h-2) selecting a user allowed to be access the file; and

h-3) setting the access authority to the file as an access authority of the user.

33. The computer readable media as recited in claim 26, wherein the step i) accessing and processing a file includes the steps of:

i-1) receiving a name of a file to be accessed;

i-2) determining whether an access authority of the file to be accessed is equal to that of the system security manager;

i-3) permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the system security manager;

i-4) determining whether the access authority of the file to be accessed is equal to that of the user trying to access thereto; and

i-5) permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the user trying to access thereto.